Pengenalan
SNI ISO/IEC 27001:2013
Sistem Manajemen Keamanan Informasi
untuk
Pengelolaan Keamanan Informasi

11 November 2021

Ramita Utami, S.Kom

Apa itu standar ?

- Sepeda motor tidak ambruk
- Secara sederhana memiliki fungsi untuk menopang beban kendaraan saat sedang parkir
- Efisiensi ruang parkir

Apa itu standar ?

- **Kepastian untuk pelanggan**
- **Jaminan kepuasan pelanggan**
- **Kemudahan ekspor**

Standar menurut UU No. 20 Tahun 2014

tentang Standardisasi dam Penilaian Kesesuaian

Standar adalah **persyaratan teknis** atau sesuatu yang **dibakukan**, termasuk **tata cara** dan **metode** yang **disusun** berdasarkan **konsensus** semua pihak/Pemerintah/keputusan internasional yang **terkait** dengan memperhatikan **syarat** keselamatan, keamanan, kesehatan, lingkungan hidup, perkembangan ilmu pengetahuan dan teknologi, pengalaman, serta perkembangan masa kini dan masa depan untuk **memperoleh manfaat** yang sebesar-besarnya.

MUTU NASIONAL

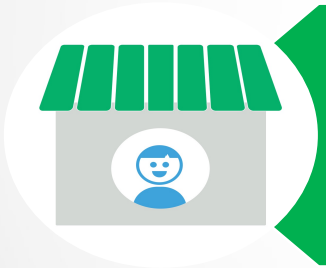
BSN BADAN STANDARDISASI NASIONAL

KAN Komite Akreditasi Nasional

Tujuan Standardisasi

sesuai UU No. 20 Tahun 2014

Meningkatkan **jaminan mutu, efisiensi produksi, daya saing nasional, persaingan usaha yang sehat** & **transparan** dalam perdagangan, kepastian usaha, dan kemampuan Pel aku Usaha, serta kemampuan **inovasi teknologi**;



Meningkatkan perlindungan kepada konsumen, Pelaku Usaha, tenaga kerja, dan masyarakat lainnya, serta negara, baik dari aspek keselamatan, keamanan, kesehatan, maupun pelestarian fungsi lingkungan hidup; dan

Meningkatkan **kepastian, kelancaran, dan efisiensi** transaksi perdagangan Barang dan/atau Jasa di dalam negeri dan luar negeri.

MUTU NASIONAL

BSN BADAN STANDARDISASI NASIONAL

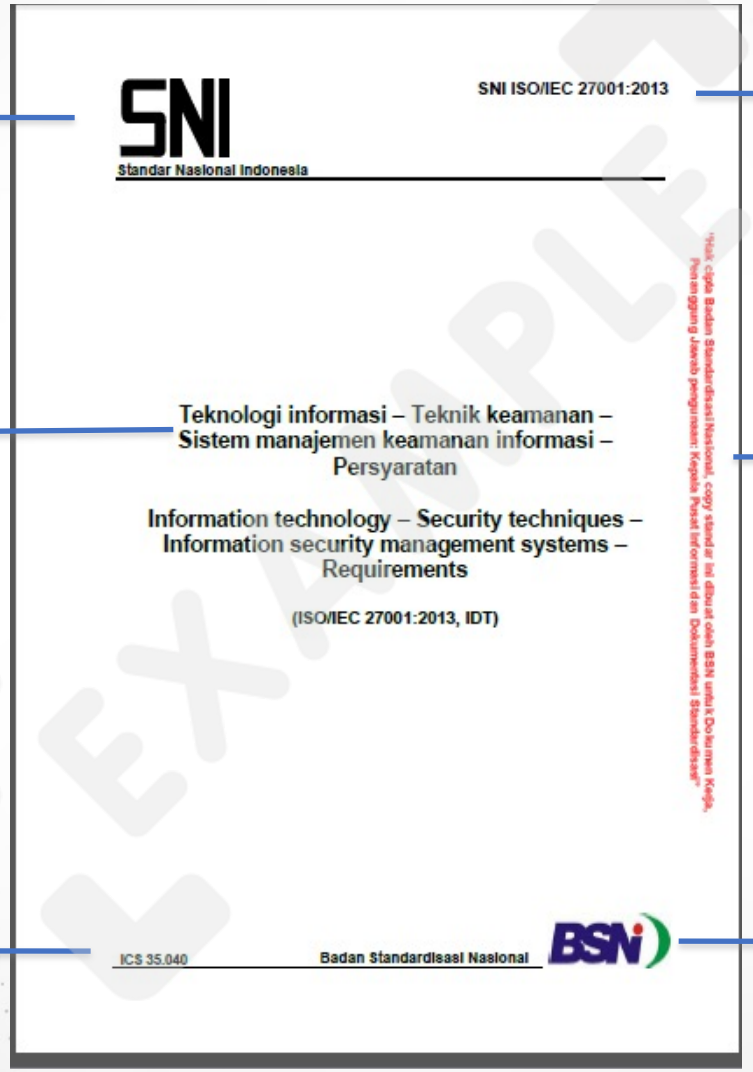
KAN Komite Akreditasi Nasional

Apa itu SNI ?

- Standar Nasional Indonesia (SNI)
- Dirumuskan oleh Komite Teknis dan Ditetapkan oleh BSN
- Diuji secara berkala
- Berawal dari sukarela, lalu bisa menjadi wajib

Jenis dan Contoh SNI

Dokumen SNI



Logo Dokumen SNI

Nomor SNI

Judul SNI

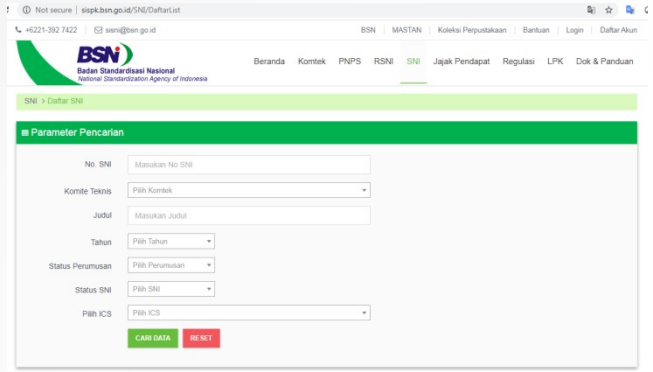
Watermark

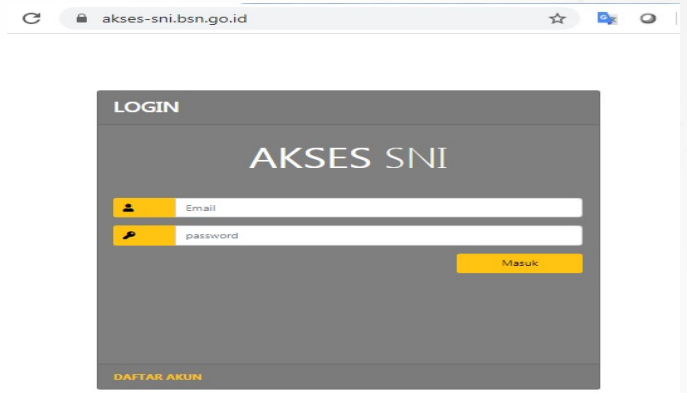
Kode International Classification Standards

Logo BSN

sispk.bsn.go.id

akses-sni.bsn.go.id





pesta.bsn.go.id

MUTU NASIONAL

BSN BADAN STANDARDISASI NASIONAL

KAN Komite Akreditasi Nasional

Apa itu Keamanan

- ✓ Keadaan bebas dari bahaya
- ✓ Bebas dari gangguan
- ✓ Terlindungi
- ✓ Tidak dapat diambil orang

- KBBI -

Apa itu Informasi

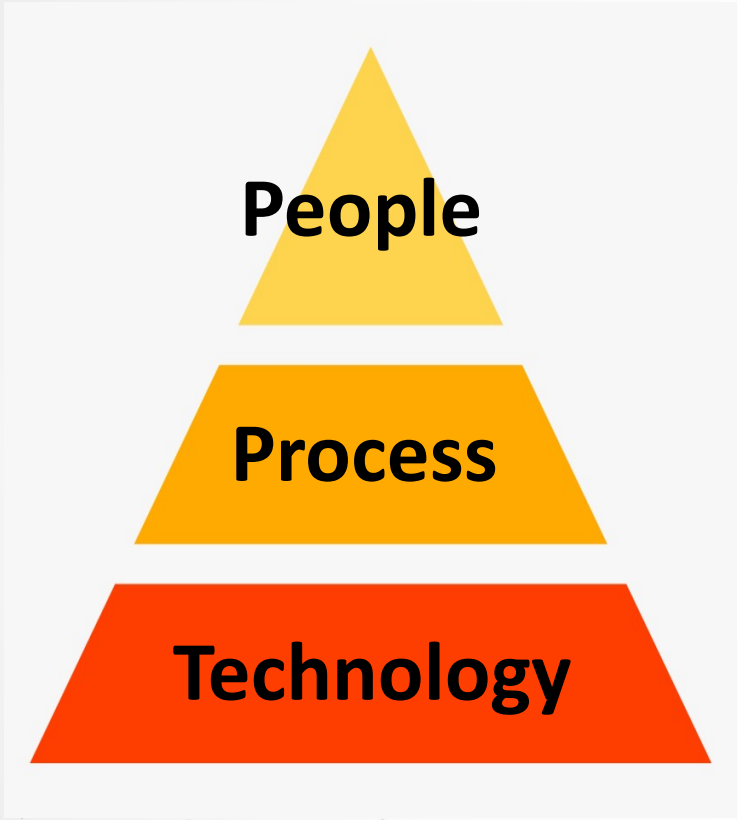
- Sesuatu (data) yang **memiliki nilai** (bisnis dan operasional) bagi organisasi.
- Sesuatu (data) yang **kritikal bagi operasional** organisasi.
- Infomasi adalah **aset**, seperti aset bisnis penting lainnya, yang memiliki nilai bagi suatu organisasi sehingga pada akhirnya perlu untuk diamankan.

Apa itu Keamanan Informasi

Keamanan Informasi **adalah** Penjagaan terhadap Kerahasiaan (**Confidentiality**), Keutuhan (**Integrity**) dan Ketersediaan (**Availability**) atas informasi.

- SNI ISO/IEC 27000:2013 -

3 Elemen yang Harus Dilindungi

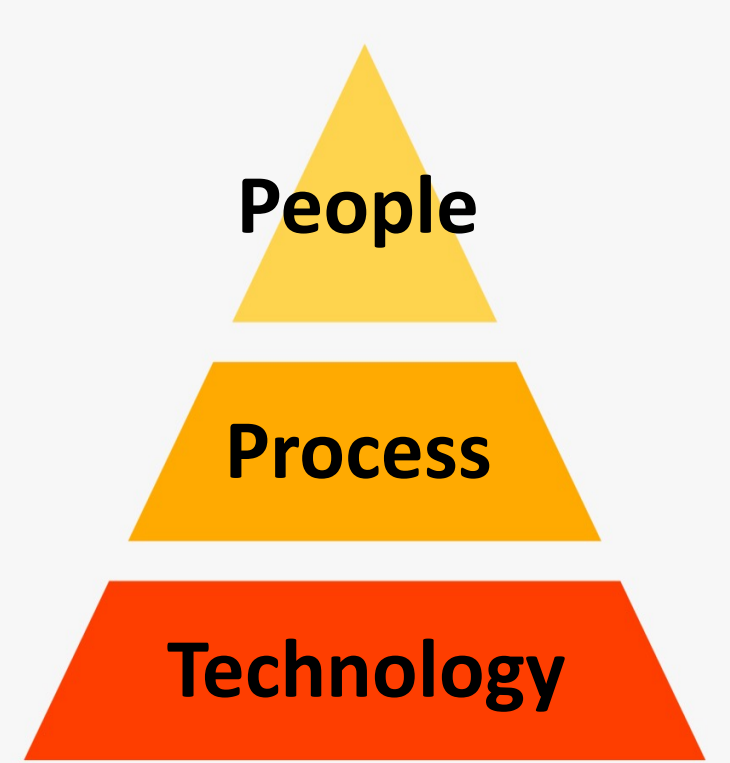


Orang atau badan yang berinteraksi dengan informasi milik organisasi.

Proses atau alur kerja merupakan langkah berulang yang diperlukan untuk mencapai tujuan organisasi.

Teknologi merupakan apa yang digunakan untuk meningkatkan apa yang dilakukan.

Contoh

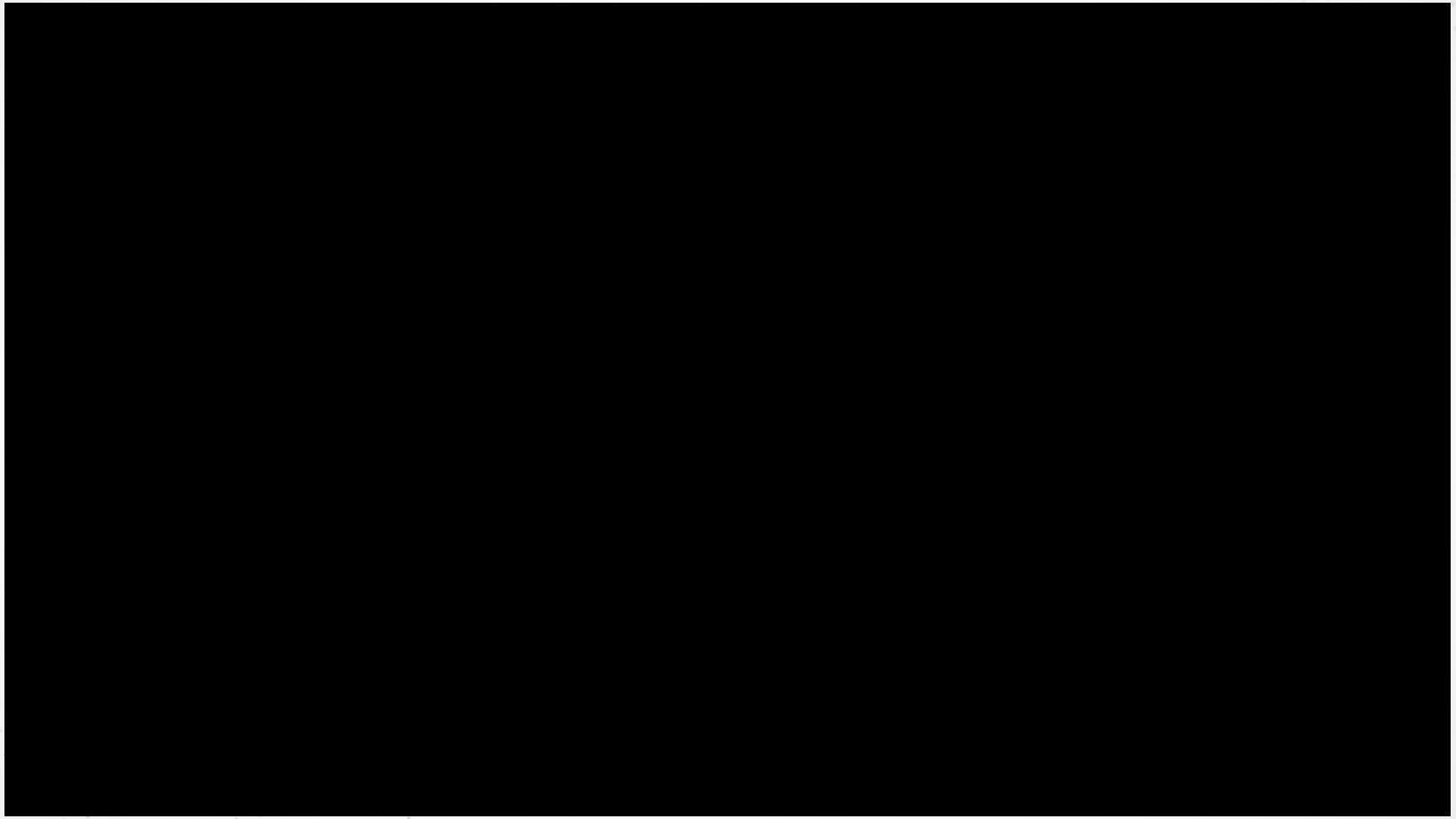


Stakeholders, Pemilik Organisasi, Pihak Manajemen, Staff / Pegawai, Vendor, Mitra Kerja, Penyedia Jasa Layanan, Konsultan, dll.

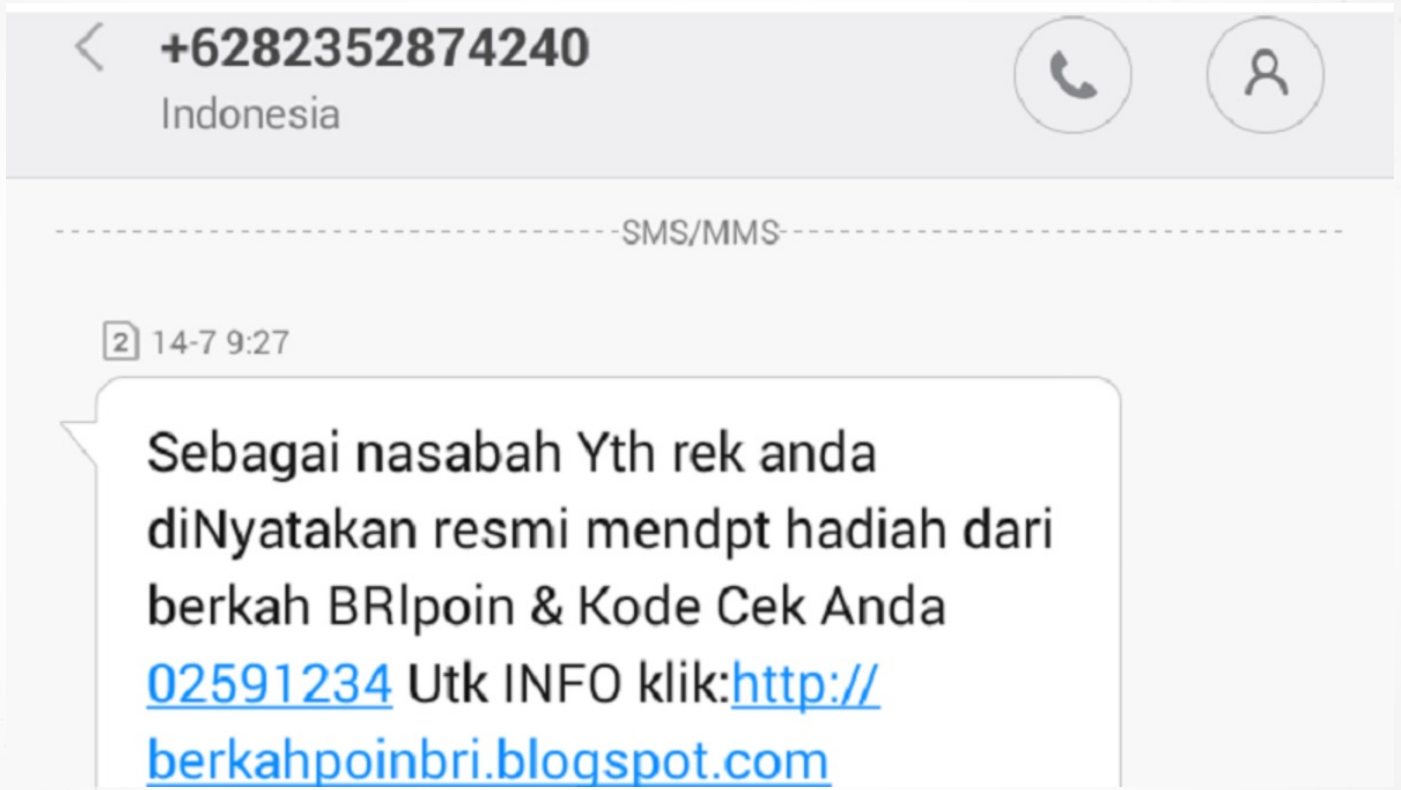
Help Desk, Pelaporan Insiden, Pemenuhan Permintaan (*Request*), Pengelolaan Akses, Pengelolaan Identitas, Pengadaan TIK, dll.

Kabel, Perangkat dan Jaringan Data/Voice, Layanan Telekomunikasi (Video Conferencing), Server, Desktop & Media Penyimpanan, Sistem Operasi, Aplikasi, dll.

Awareness

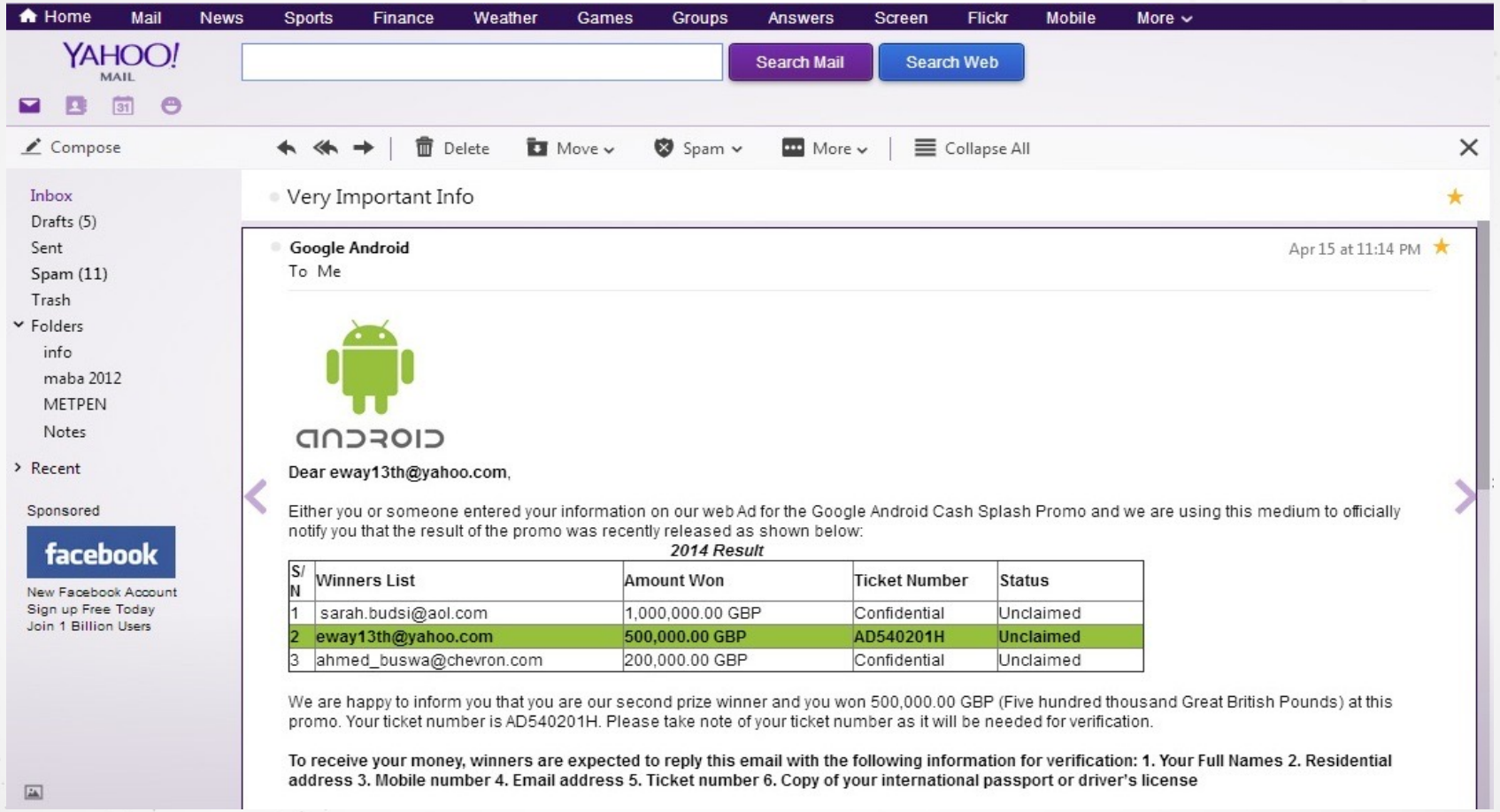


Contoh Kasus



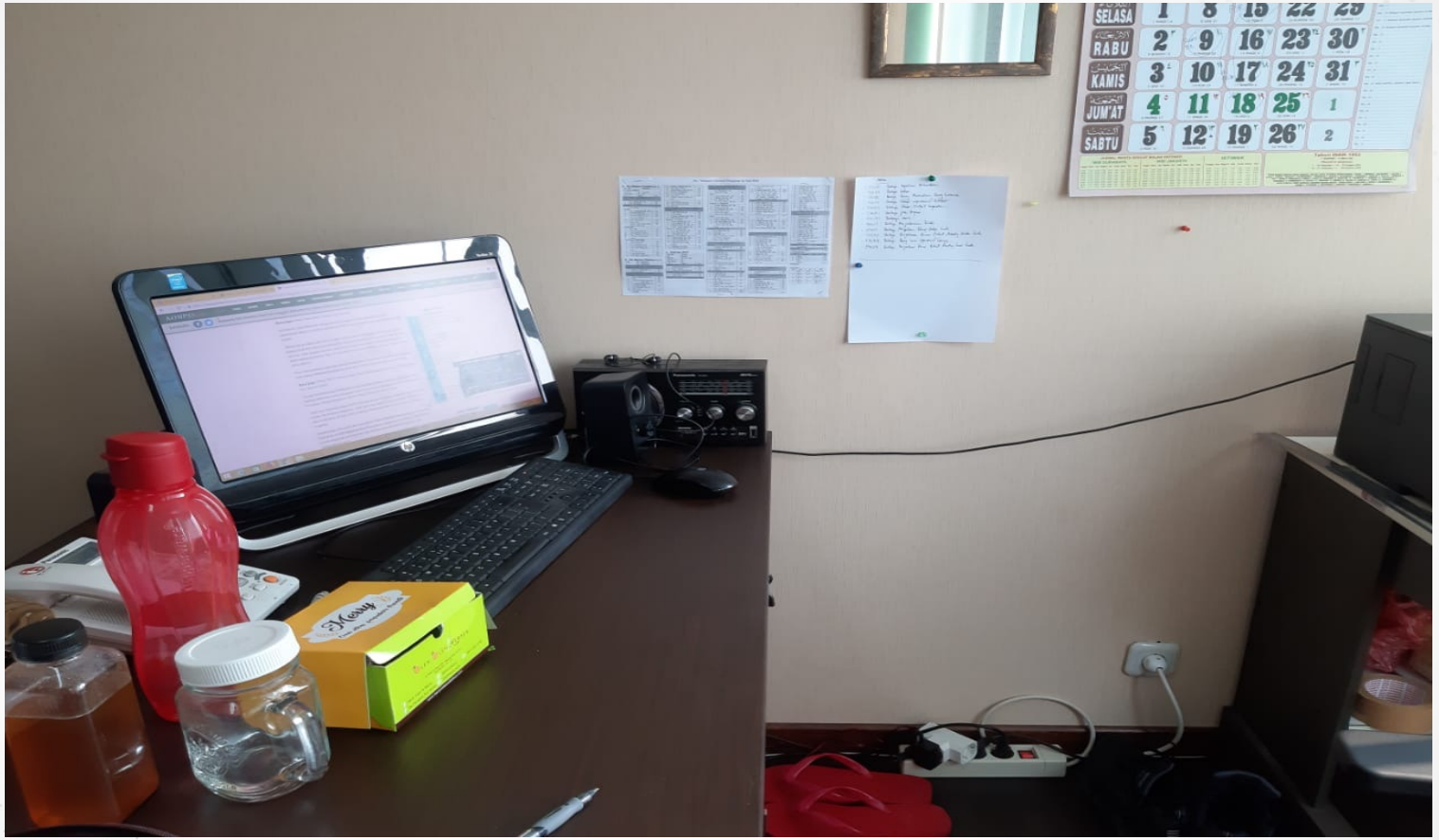
SMS Penipuan

Contoh Kasus



Email spam

Contoh Kasus



Sistem Manajemen Keamanan Informasi (SMKI)

adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Ini termasuk orang, proses dan sistem TI (Teknologi Informasi) dengan menerapkan proses manajemen resiko.

Apa itu SNI ISO/IEC 27001:2013 ?

MUTU NASIONAL

BSN BADAN STANDARDISASI NASIONAL

KAN Komite Akreditasi Nasional

ISO yaitu **organisasi internasional** untuk standardisasi yang menetapkan **standar internasional** di bidang **industrial** dan **komersial** dunia dimana tujuan pembentukannya untuk **meningkatkan perdagangan antar negara-negara** di dunia.

IEC adalah **organisasi standardisasi internasional** yang **menyusun** dan **menerbitkan standar-standar** internasional untuk seluruh **bidang elektrik**, **elektronik** dan **teknologi** yang terkait atau bidang **teknologi elektro** (electrotechnology).

ISO/IEC 27001:2013 adalah standar (panduan) keamanan informasi yang diterbitkan oleh ISO dan IEC yang menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan SMKI.

Versi ini adalah **versi terbaru** dari versi sebelumnya ISO/IEC 27001:2005.

SNI ISO/IEC 27001:2013 adalah standar adopsi dari ISO/IEC 27001:2013 yang dikeluarkan oleh **BSN**

ISO 27000 Family of International Standards

Provides the best practice recommendations on InfoSec management, risks and controls within the context of an overall ISMS.

ISO 27000: Overview and Vocabulary (2014)

ISO 27001: ISMS Requirements (2013)

ISO 27002: Code of Practice (2013)

ISO 27003: ISMS Implementation Guidance (2010)

ISO 27004: ISM Measurement (2009)

ISO 27005: InfoSec Risk Management (2011)

ISO 27006: Requirements for Bodies Providing Audit and Certification of ISMS (2011)

ISO 27007 – 27008: Guidelines for Auditing InfoSec Controls (2011)

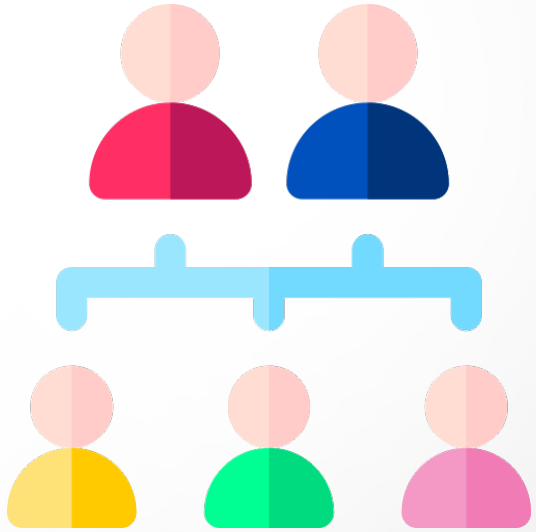
ISO 27014: Governance of InfoSec (2013)

ISO 27015: ISM Guidelines for Financial Services (2012)

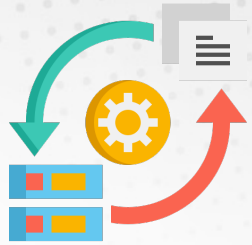
- www.iso.org

Keluarga

ISO/IEC 27001:2013



Perubahan



ISO/IEC 27001:2005	ISO/IEC 27001:2013
132 shall statements section **4 to 8**	**125 shall** statements section **4 to 10**
Annex A	
11 clauses	**14** clauses
39 categories	**35** categories
133 controls	**114** controls

Struktur
SNI ISO/IEC 27001:2013

Terdiri dari **10 klausul** dan lampiran **Annex** (14 Kelompok Domain & 114 Kendali / Kontrol)

Klausul 4 - 10 tidak dapat dikecualikan (**wajib**) dalam sertifikasi SNI ISO/IEC 27001:2013

1. Ruang Lingkup

2. Acuan Normatif

3. Istilah dan Definisi

4. Konteks Organisasi

4.1 Memahami organisasi & kontek
4.2 Memahami kebutuhan
4.3 Penentuan ruang lingkup SMKI
4.4 SMKI

5. Kepemimpinan

5.1 Kepemimpinan & komitmen
5.2 Kebijakan
5.3 Peran organisasi, tanggung jawab & wewenang

6. Perencanaan

6.1 Tindakan untuk menangani resiko & peluang
6.2 Sasaran keamanan informasi & perencanaan untuk mencapaianya

7. Dukungan

7.1 Sumberdaya
7.2 Kompetensi
7.3 Kepedulian
7.4 Komunikasi
7.5 Informasi terdokumentasi

8. Operasi

8.1 Perencanaan & pengendalian operasional
8.2 Penilaian resiko keamanan informasi
8.3 Penanganan resiko keamanan informasi

9. Evaluasi Kinerja

9.1 Pemantauan, pengukuran, analisis & evaluasi
9.2 Audit internal
9.3 Reviu manajemen

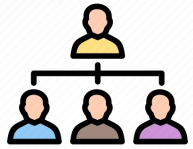
10. Perbaikan

10.1 Ketidaksesuaian & tindakan korektif
10.2 Perbaikan berkelanjutan

Klausul wajib

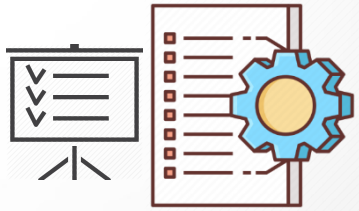
SNI ISO/IEC 27001:2013

Klausul 4
- Konteks Organisasi



Klausul 5
- Kepemimpinan

Klausul 6
- Perencanaan



Klausul 7
- Dukungan

Klausul wajib

SNI ISO/IEC 27001:2013

Klausul 8

- Operasi

Klausul 9

- Evaluasi Kinerja

Klausul 10

- Perbaikan

Lampiran Anex

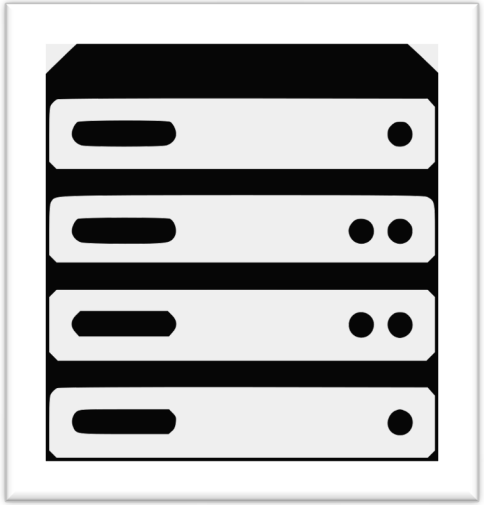
SNI ISO/IEC 27001:2013

SNI ISO/IEC 27001:2013 Control Point and Control Objective		
Annex	**Deskripsi**	**total Kontrol**
A5	Kebijakan Keamanan Informasi	**2**
A6	Organisasi Keamanan informasi	**7**
A7	Keamanan Sumber Daya Manusia	**6**
A8	Manajemen Aset	**10**
A9	Kendali Akses	**14**
A10	Kriptografi	**2**
A11	Keamanan Fisik dan Lingkungan	**15**
A12	Keamanan Operasi	**14**
A13	Keamanan Komunukasi	**7**
A14	Akuisisi, Pengembangan dan Perawatan Sistem	**13**
A15	Hubungan Pemasok	**5**
A16	Manajemen Insiden Keamanan Informasi	**7**
A17	Aspek Keamanan Informasi dari Manajemen Keberlangsungan	**4**
A18	Kesesuaian	**8**
Total Kontrol		**114**

Implementasi Kendali (Anex)

Pengelolaan

Email



Ruang Server

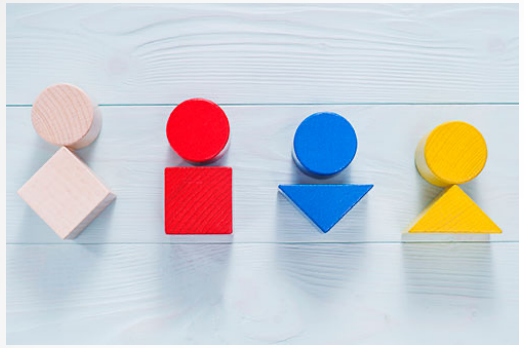
Akses

Pengelolaan Email

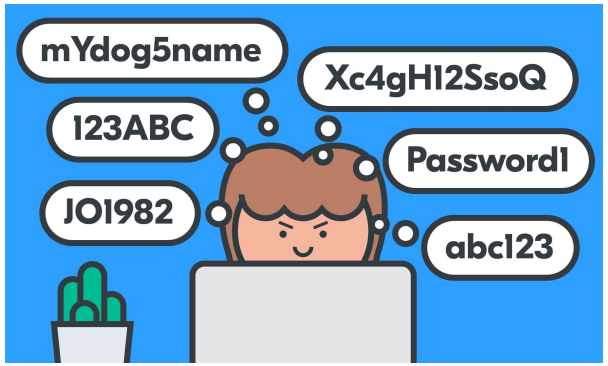
A8 Manajemen Aset

A9 Kendali Akses

Best Practice



Pisahkan email

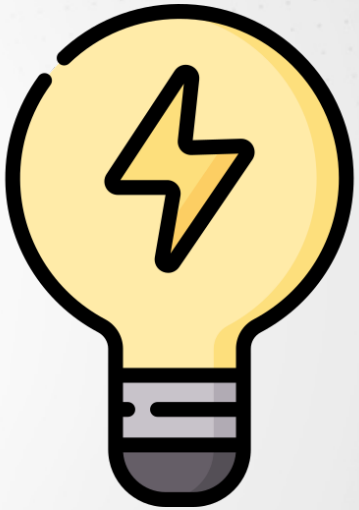


Password berbeda

Logout &
clear history

Pengelolaan Ruang Server

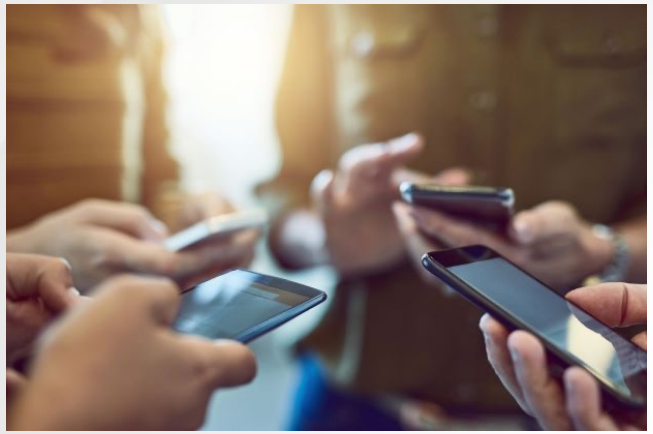
Pengelolaan Ruang Server



Pengelolaan Akses

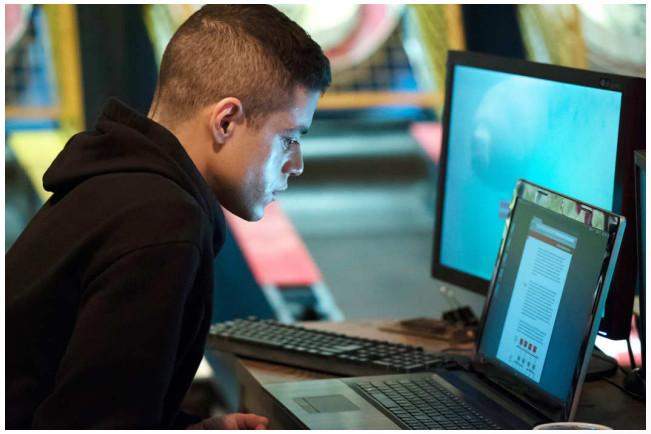
- Pengguna tertelusur
- Mencegah pihak tidak berwenang

Pengelolaan Akses

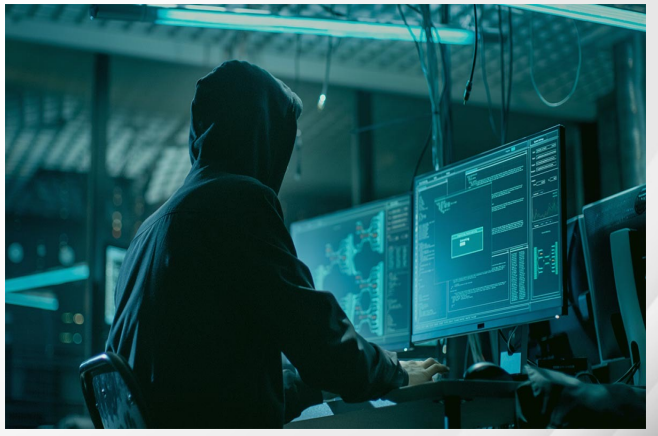


User

Web Admin



Administrator



Super Admin

A11 Keamanan Fisik dan Lingkungan

Ruang Kerja

Ruang Server

A11 Keamanan Fisik dan Lingkungan

Ruang Penerimaan Tamu

Ruang Penyimpanan

Ruang Penerimaan Tamu

Isi Buku Tamu

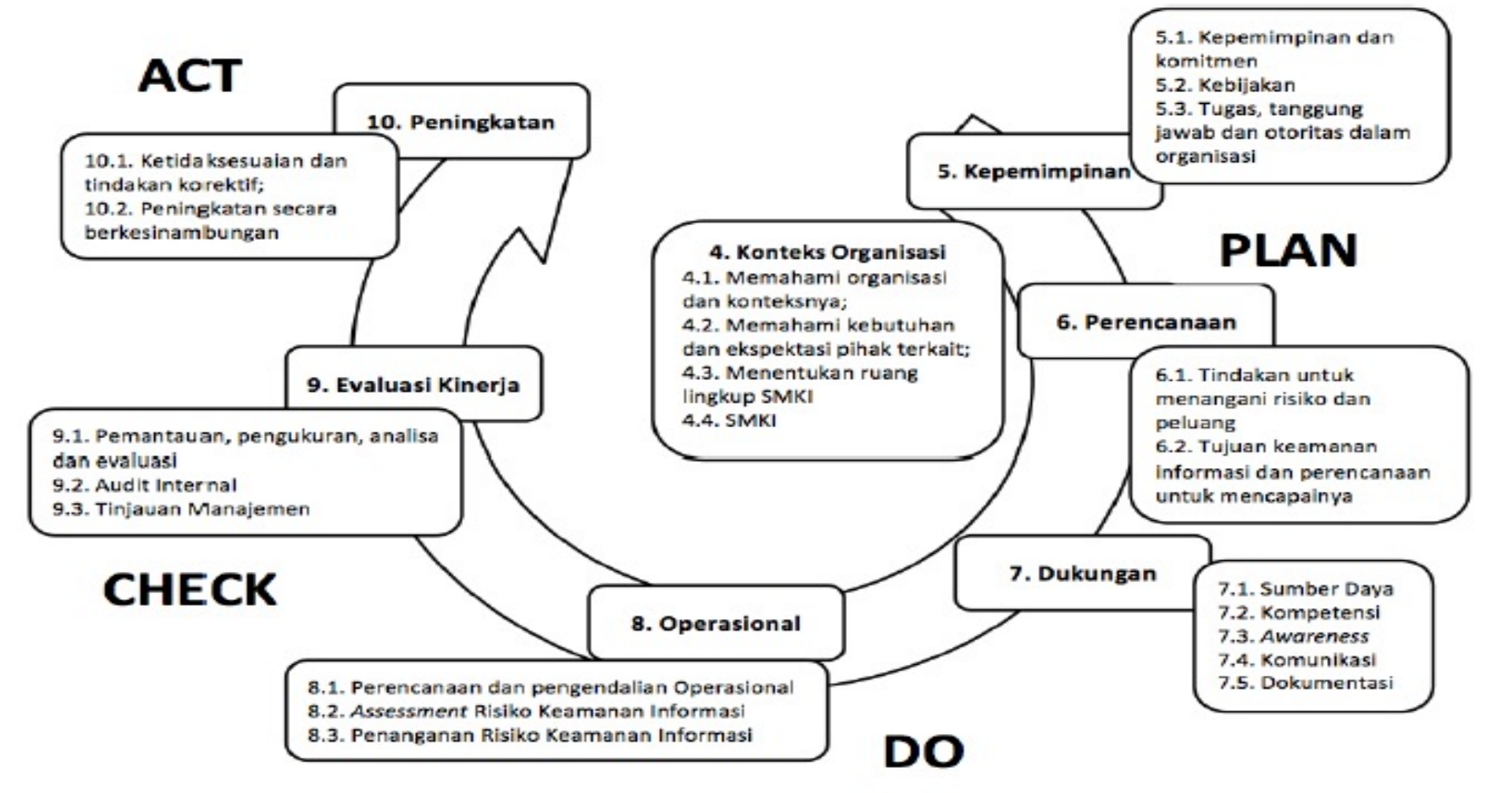
Kartu Akses

Ruang Server

Lock System

Log Access

Siklus PDCA terkait klausul SNI ISO/IEC 27001:2013



Sertifikat SNI ISO/IEC 27001:2013

CERTIFICATE

SUCOFINDO

Certificate No. ISMS 00005

SUCOFINDO INTERNATIONAL CERTIFICATION SERVICES

Graha Sucofindo B1 Floor - Jl. Raya Pasar Minggu Kav. 34 Jakarta 12780
Phone : +62-21-7983666 ext. 1021; Fax : +62-21-7987015 / 7987029; Email : cs.sics@sucofindo.co.id

Menyatakan bahwa
Certify that

BADAN STANDARDISASI NASIONAL (BSN)

Gedung I BPPT
Jl. M.H. Thamrin No. 8, Jakarta Pusat - INDONESIA

telah menerapkan sistem manajemen keamanan informasi yang memenuhi
has implemented information security management system that comply with

SNI ISO/IEC 27001:2013
Information Security Management Systems-Requirements
Persyaratan-Sistem Manajemen Keamanan Informasi

Ruang lingkup sertifikasi :
The scope of certification :

Sistem Manajemen Keamanan Informasi pada Pusat Data dan Sistem Informasi.

Statement of Applicability Ver 1.0 date. 16 Juli 2019

Keuntungan penerapan SNI ISO/IEC 27001:2013

- Membuat **pengaruh positif** dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain.
- Memastikan bahwa **organisasi memiliki kontrol terkait keamanan** informasi terhadap lingkungan proses bisnisnya yang mungkin menimbulkan risiko atau gangguan.
- **Dapat** digabung atau **dikombinasikan** dengan **sistem manajemen lainnya** seperti SNI ISO 9001, SNI ISO 14000, SNI ISO 20000, SNI ISO 37001, SNI ISO 38500, ITIL, COBIT, Sistem Manajemen SPBE, dll.
- Salah satu **standar pengamanan** informasi yang **diakui di seluruh dunia**.
- **Patuh** terhadap **hukum** dan undang-undang seperti UU ITE, PermenPANRB No.59 Tahun 2020, dll.
- **Meningkatkan awareness** terhadap keamanan informasi pada pegawai/karyawan.

Landasan Pelaksanaan Evaluasi SPBE

PERPRES 95/2018

PERMENPANRB 5/2018

Pedoman **Evaluasi SPBE** digunakan sebagai panduan dalam melakukan penilaian/evaluasi SPBE untuk **mengukur kemajuan pelaksanaan Sistem Pemerintahan Berbasis Elektronik** pada Instansi Pusat dan Pemerintah Daerah.

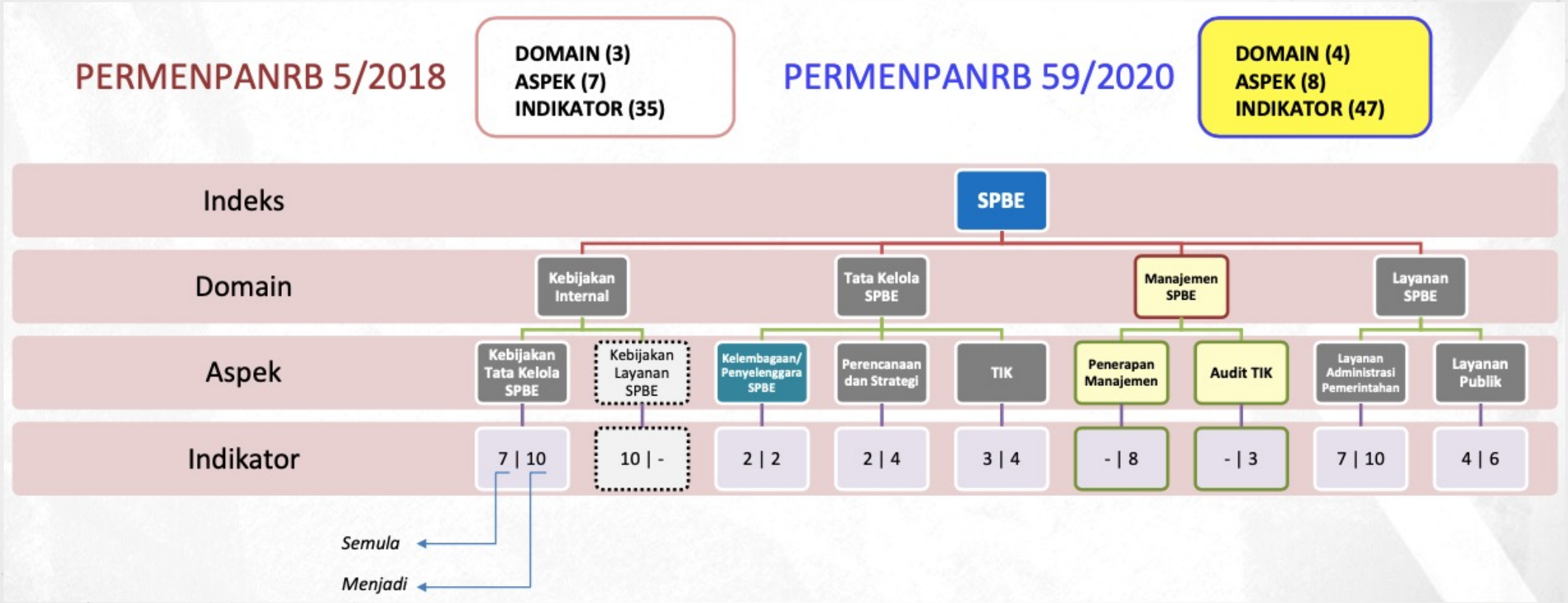
REVISI TERHADAP PERMENPANRB 5/2018

PermenPANRB No. 5 Tahun 2018 terbit lebih dulu (9 bulan 11 hari) sebelum Perpres 95 Tahun 2018 terbit.

Beberapa **amanat** Perpres 95 Tahun 2018 yang **belum terakomodasi** dalam PermenPANRB No. 5 Tahun 2018, antara lain:

a. Arsitektur SPBE (Pasal 6–12)
b. Peta Rencana SPBE (Pasal 13–19)
c. Jaringan Intra Pemerintah (Pasal 32)
d. Sistem Penghubung Layanan (Pasal 33)
e. Pembangunan Aplikasi Terpadu (Pasal 34–39)
f. Keamanan SPBE (Pasal 40–41)
g. Manajemen SPBE: Manajemen Risiko, Manajemen Data, Manajemen Aset TIK, Manajemen Keamanan Informasi, Manajemen Layanan, Manajemen SDM SPBE, Manajemen Perubahan, Manajemen Pengetahuan (Pasal 46–54)
h. Audit TIK: Audit Aplikasi, Audit Infrastruktur, Audit Keamanan (Pasal 55–58)

Struktur Penilaian



Metodologi Evaluasi

Mengukur tingkat kematangan (skala 1 - 5) pada indikator penilaian di domain Kebijakan, Tata Kelola, Manajemen, dan Layanan SPBE

Kebijakan	Kebijakan Tata Kelola SPBE	•Indikator kebijakan internal yang mendukung penerapan tim koordinasi SPBE, perencanaan, strategi, manajemen, dan Audit TIK SPBE.
Tata Kelola	Perencanaan Strategis SPBE	•Indikator terkait arsitektur, peta rencana, anggaran, dan proses bisnis SPBE.
	Teknologi Informasi dan Komunikasi	•Indikator kematangan pembangunan jaringan intra pemerintah, pusat data, dan sistem penghubung layanan SPBE.
	Penyelenggara SPBE	•Indikator pelaksanaan tugas Tim Koordinasi SPBE dan kolaborasi penerapan SPBE.
Manajemen	Penerapan Manajemen SPBE	•Indikator manajamen risiko, keamanan informasi, data, aset, SDM, pengetahuan, perubahan, dan Layanan SPBE.
	Audit TIK	•Indikator audit infrastruktur, aplikasi, dan keamanan SPBE
Layanan	Layanan Administrasi Pemerintahan	•Indikator layanan perencanaan, penganggaran, keuangan, pengadaan, kepegawaian, kearsipan, pengelolaan BMN, pengawasan, akuntabilitas, kinerja.
	Layanan Publik	•Indikator layanan pengaduan publik, data terbuka, JDIH, dan layanan publik unggulan lain.

Tingkat Kematangan Kebijakan, Tata Kelola, dan Manajemen

1 Rintisan	2 Terkelola	3 Terdefinisi
4 Terpadu dan Terukur	5 Optimum	

Tingkat Kematangan Layanan

1 Informasi	2 Interaksi	3 Transaksi
4 Kolaborasi	5 Optimum	

MUTU NASIONAL

BSN BADAN STANDARDISASI NASIONAL

KAN Komite Akreditasi Nasional

Konsep Kematangan
Keamanan Informasi SPBE

PENYUSUNAN KEBIJAKAN

PENERAPAN

AUDIT

Tingkat Kematangan
Manajemen Keamanan Informasi SPBE

Aspek 1 – Kebijakan Internal Tata Kelola SPBE

Indikator 8

Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi

Aspek 5 – Penerapan Manajemen SPBE

Indikator 22

Tingkat Kematangan Penerapan Manajemen Keamanan Informasi

Aspek 6– Pelaksanaan Audit TIK

Indikator 31

Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

Tingkat Kematangan
Kebijakan Internal Manajemen Keamanan Informasi

Tingkat	Kriteria
1	Konsep kebijakan internal terkait Manajemen Keamanan Informasi belum atau telah tersedia.
2	Kebijakan internal terkait Manajemen Keamanan Informasi telah ditetapkan. Kondisi: Kebijakan internal terkait Manajemen Keamanan Informasi belum mengatur secara lengkap mengenai cakupan Manajemen Keamanan Informasi (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
3	Kriteria tingkat 2 telah terpenuhi dan kebijakan internal terkait Manajemen Keamanan Informasi mengatur seluruh cakupan Manajemen Keamanan Informasi secara lengkap (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
4	Kriteria tingkat 3 telah terpenuhi, dan kebijakan internal terkait Manajemen Keamanan Informasi telah mengatur penerapan untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah. Selain itu, kebijakan internal terkait Manajemen Keamanan Informasi telah direviu dan dievaluasi secara periodik.
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi kebijakan internal terkait Manajemen Keamanan Informasi telah ditindaklanjuti dengan kebijakan baru.

Tingkat Kematangan Penerapan Manajemen Keamanan Informasi

Tingkat	Kriteria
1	Pengendalian Keamanan Informasi belum atau telah tersedia dalam tahap pembangunan.
2	Pengendalian Keamanan Informasi telah tersedia. Kondisi: Pengendalian Keamanan Informasi telah dilaksanakan pada sebagian unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah.
3	Kriteria tingkat 2 telah terpenuhi dan pengendalian Keamanan Informasi telah dilaksanakan pada seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah dengan berdasarkan Risiko SPBE.
4	Kriteria tingkat 3 telah terpenuhi dan pengendalian Keamanan Informasi dilakukan melalui strategi Keamanan Informasi yang ditetapkan oleh Tim Koordinasi SPBE Instansi Pusat/Pemerintah Daerah. Selain itu, pengendalian Keamanan Informasi telah dilakukan reviu dan evaluasi secara periodik.
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi pengendalian Keamanan Informasi ditindaklanjuti melalui perbaikan penerapan proses pengendalian Keamanan Informasi.

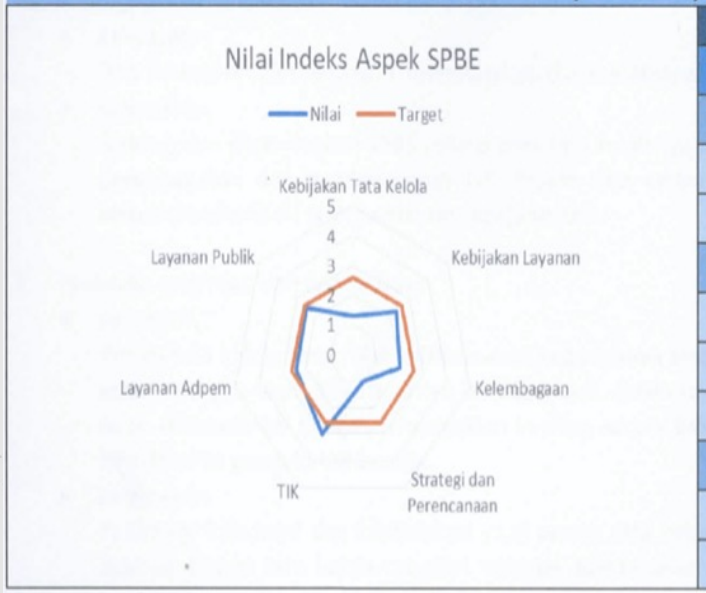
Tingkat Kematangan
Pelaksanaan Audit Keamanan SPBE

Tingkat	Kriteria
1	Kegiatan Audit Keamanan SPBE belum atau telah dilaksanakan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa perencanaan yang berkesinambungan.
2	Kriteria tingkat 1 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan perencanaan yang berkesinambungan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa pedoman Audit Keamanan.
3	Kriteria tingkat 2 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan pedoman Audit Keamanan. Kondisi: kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi internal Instansi Pusat/Pemerintah Daerah.
4	Kriteria tingkat 3 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi eksternal yang memiliki sertifikasi auditor TIK/Sistem Keamanan Informasi.
5	Kriteria tingkat 4 telah terpenuhi dan hasil audit Keamanan SPBE telah ditindaklanjuti melalui perbaikan penerapan Keamanan SPBE.

History Nilai SPBE BSN

2018 (Cukup)

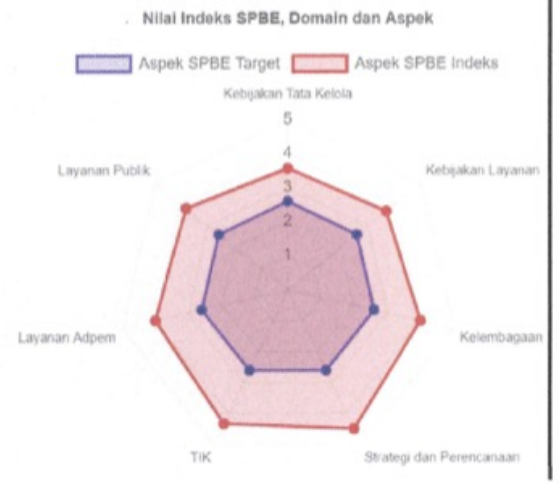
Nilai Indeks SPBE, Domain, dan Aspek



Indeks	Nilai
SPBE	2,27
Domain Kebijakan SPBE	1,88
Kebijakan Tata Kelola SPBE	1,29
Kebijakan Layanan SPBE	2,30
Domain Tata Kelola	2,14
Kelembagaan	2,00
Strategi & Perencanaan	1,00
TIK	3,00
Domain Layanan SPBE	2,45
Administrasi Pemerintahan	2,43
Pelayanan Publik	2,50

2019 (Sangat Baik)

NILAI INDEKS SPBE, DOMAIN DAN ASPEK



Nama Instansi
Badan Standardisasi Nasional

K/L/D	:	LPNK
Daerah	:	Pusat
Indeks SPBE	:	**3.99**
Predikat SPBE	:	Sangat Baik
Domain Kebijakan SPBE	:	**3.65**
➥ Kebijakan Tata Kelola SPBE	:	3.57
➥ Kebijakan Layanan SPBE	:	3.7
Domain Tata Kelola	:	**4.29**
➥ Kelembagaan	:	4.00
➥ Strategi dan Perencanaan	:	4.5
➥ TIK	:	4.33
Domain Layanan SPBE	:	**3.94**
➥ Administrasi Pemerintahan	:	4.00
➥ Pelayanan Publik	:	3.83

MUTU NASIONAL

BSN BADAN STANDARDISASI NASIONAL

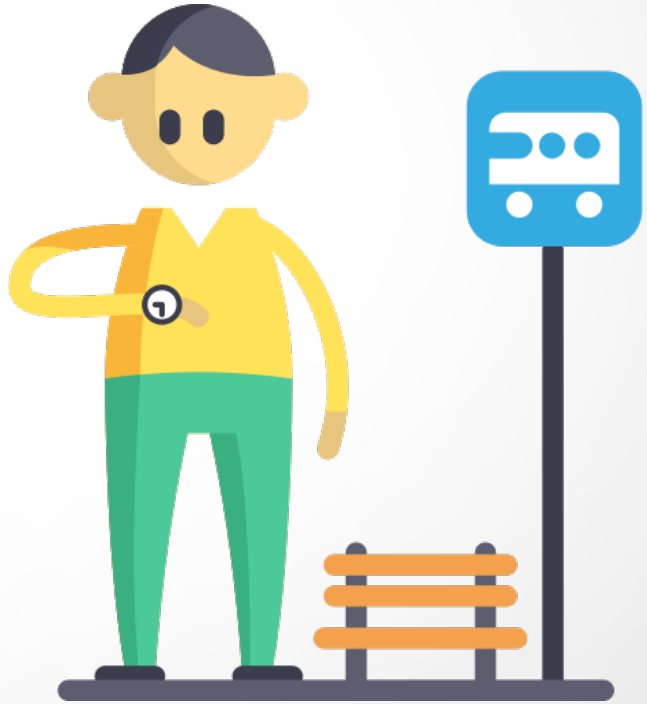
KAN Komite Akreditasi Nasional

Pengajuan Nilai SPBE 2021

Penilaian Mandiri

Nama Instansi	
Badan Standardisasi Nasional	
K/L/D	: Lembaga Pemerintah Non Kementerian
Indeks SPBE	: **4.73**
Predikat SPBE	: **Memuaskan**
Domain Kebijakan SPBE	: **5.00**
Kebijakan Internal terkait Tata Kelola SPBE	: 5.00
Domain Tata Kelola SPBE	: **4.60**
Perencanaan Strategis SPBE	: 5.00
Teknologi Informasi dan Komunikasi	: 4.25
Penyelenggara SPBE	: 4.50
Domain Manajemen SPBE	: **4.64**
Penerapan Manajemen SPBE	: 4.50
Audit TIK	: 5.00
Domain Layanan SPBE	: **4.75**
Layanan Administrasi Pemerintahan Berbasis Elektronik	: 4.80
Layanan Publik Berbasis Elektronik	: 4.67

Penilaian Final ?



BADAN STANDARDISASI NASIONAL

KAN Komite Akreditasi Nasional

TERIMA KASIH

bsn_sni Badan Standardisasi Nasional www.bsn.go.id

MUTU NASIONAL